#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Takayuki SUGAHARA et al.	
Serial No. 09/740,843	Art Unit: 2131
Filed: December 21, 2000	Examiner:
For: METHOD AND APPARATUS FOR DECRYPTING CONTENTS INFORMATION	Atty Docket: 0102/0151

SUBMISSION OF PRIORITY DOCUMENTS

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Attached hereto please find a certified copy of applicants' Japanese application No. 2000-037625 filed February 16, 2000.

Applicants request the benefit of said February 16, 2000 filing date for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

Louis Woo, RN 31,730
Law Offices of Louis Woo
1901 North Fort Myer Drive, Suite 501
Arlington, VA 22209
(703) 522-8872

Date: March 16 2001

U4-0027-TH

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　２月１６日

出願番号
Application Number: 特願２０００－０３７６２５

出願人
Applicant (s): 日本ビクター株式会社

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０７４２３

【書類名】　特許願

【整理番号】　412000053

【提出日】　平成12年 2月16日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　1/00

G09C　1/00

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　菅原　隆幸

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　日暮　誠司

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　守隨　武雄

【電話番号】　045-450-2423

【手数料の表示】

【予納台帳番号】　003654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　コンテンツ情報復号化方法及びコンテンツ情報復号化装置

【特許請求の範囲】

【請求項１】

暗号化されたコンテンツ情報を復号するための第１の鍵を生成するために必要な鍵生成情報を得て前記第１の鍵を生成し、前記暗号化されたコンテンツ情報を復号する復号化方法において、

前記鍵生成情報の少なくとも一部と、少なくとも認証値とから所定の関数により外部で生成された伝送用鍵のもとになる情報が供給され、

復号化側の復号化装置の固有ID情報と前記認証値とから生成された発行ID情報が供給され、

前記固有ID情報と前記発行ID情報とから前記認証値を生成し、

少なくともこの生成した認証値と前記伝送用鍵のもとになる情報とから所定の逆関数により前記鍵生成情報の少なくとも一部を得る、

ことを特徴とするコンテンツ情報復号化方法。

【請求項２】

第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、第２の鍵のもとになる情報から生成された第２の鍵を用いて前記第１の鍵のもとになる情報の少なくとも一部を暗号化した暗号化第１の鍵のもとになる情報と、前記第２の鍵のもとになる情報と少なくとも認証値とから所定の関数により生成された伝送用鍵のもとになる情報と、復号化側の復号化装置の固有ID情報と前記認証値とから生成された発行ID情報と、

を用いて前記コンテンツ情報を復号する方法であって、

前記固有ID情報と前記発行ID情報とから前記認証値を生成し、

少なくともこの生成した認証値と前記伝送用鍵のもとになる情報とをもとに、所定の逆関数により前記第２の鍵のもとになる情報を生成し、

この生成された第２の鍵のもとになる情報を用いて前記第２の鍵を生成し、この第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の

鍵のもとになる情報を得、

この第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得る、

ことを特徴とするコンテンツ情報復号化方法。

【請求項３】

暗号化されたコンテンツ情報を復号するための第１の鍵を生成するために必要な鍵生成情報を外部から得て前記第１の鍵を生成し、前記暗号化されたコンテンツ情報を復号する復号化装置において、

所定の認証値とこの復号化装置の固有ID情報とから生成された発行ID情報が供給され、前記固有ID情報と前記発行ID情報とから前記認証値を生成する認証値生成手段と、

前記鍵生成情報の少なくとも一部と少なくとも前記認証値とから所定の関数により外部で生成された伝送用鍵のもとになる情報が供給されると共に、少なくとも前記認証値生成手段で生成された認証値が供給され、所定の逆関数により前記鍵生成情報の少なくとも一部を生成する演算手段と、

を設けたことを特徴とするコンテンツ情報復号化装置。

【請求項４】

第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、第２の鍵のもとになる情報から生成された第２の鍵を用いて前記第１の鍵のもとになる情報の少なくとも一部を暗号化した暗号化第１の鍵のもとになる情報と、前記第２の鍵のもとになる情報と少なくとも認証値とから所定の関数により生成された伝送用鍵のもとになる情報と、この復号化装置の固有ID情報と前記認証値とから生成された発行ID情報と、

を用いて前記コンテンツ情報を復号する復号化装置であって、

前記固有ID情報と前記発行ID情報とから前記認証値を生成する認証値生成手段と、

少なくともこの生成した認証値と前記伝送用鍵のもとになる情報とをもとに、所定の逆関数により前記第２の鍵のもとになる情報を生成する第２の鍵情報生成手段と、

この生成された第２の鍵のもとになる情報を用いて前記第２の鍵を生成し、この第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得る第１の鍵情報復号化手段と、

この復号された第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得るコンテンツ情報復号化手段と、

を設けたことを特徴とするコンテンツ情報復号化装置。

【請求項５】

前記認証値生成手段に供給すべき前記発行ID情報をユーザー自身が入力するための発行ID情報入力手段を設けたことを特徴とする請求項３または４記載のコンテンツ情報復号化装置。

【請求項６】

前記発行ID情報は、暗号化コンテンツ情報供給側において、復号化側から供給された復号化装置の固有ID情報が正規の復号化装置の固有ID情報であるとの認定後に発行され復号化側に供給されるものであることを特徴とする請求項１記載のコンテンツ情報復号化方法、または請求項２記載のコンテンツ情報復号化方法、または請求項３記載のコンテンツ情報復号化装置、または請求項４記載のコンテンツ情報復号化装置、または請求項５記載のコンテンツ情報復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツ鍵とそのコンテンツ鍵を用いて暗号化された暗号化コンテンツ情報を再生（復号）するコンテンツ情報復号化方法、及び復号化装置に関するものである。そして、この発明は、特にコンテンツ情報を正規の制限下においてのみ的確に再生（復号）することを可能とするコンテンツ情報復号化方法、及び復号化装置を提供することを目的としている。

【０００２】

【従来の技術】

暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのディ

ジタルデータを配信する有用な方法として、特開平１０－２６９２８９のディジタルコンテンツ配布管理方法、ディジタルコンテンツ再生方法及び装置がある。この発明では、ディジタルコンテンツの配布側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信する。そして、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。

【０００３】

また、特開平１０－２８３２６８の情報記記録媒体、記録装置、情報伝送システム、暗号解読装置では、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が追加記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままＨＤＤや光ディスクにコピーして不正使用をすることを防止しするようにしている。

【０００４】

【発明が解決しようとする課題】

しかし、上記従来の方式では、暗号化コンテンツ情報の再生（復号）に制限を加えて、正規の条件下以外の不正な再生（復号）を防止するようにしているが、その制限情報は第三者により容易に変更することが可能であり、不正な条件下での再生（復号）を的確に防止することが難しかった。

この発明は、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするコンテンツ情報復号化方法、及び復号化装置を提供することを目的としている。

【０００５】

【課題を解決するための手段】

そこで、上記課題を解決するために本発明は、下記の各方法・装置を提供するものである。

（１）　暗号化されたコンテンツ情報を復号するための第１の鍵を生成するために必要な鍵生成情報を得て前記第１の鍵を生成し、前記暗号化されたコンテンツ情報を復号する復号化方法において、

前記鍵生成情報の少なくとも一部と、少なくとも認証値とから所定の関数により外部で生成された伝送用鍵のもとになる情報が供給され、

復号化側の復号化装置の固有ID情報と前記認証値とから生成された発行ID情報が供給され、

前記固有ID情報と前記発行ID情報とから前記認証値を生成し、

少なくともこの生成した認証値と前記伝送用鍵のもとになる情報とから所定の逆関数により前記鍵生成情報の少なくとも一部を得る、

ことを特徴とするコンテンツ情報復号化方法。

（２）　第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、第２の鍵のもとになる情報から生成された第２の鍵を用いて前記第１の鍵のもとになる情報の少なくとも一部を暗号化した暗号化第１の鍵のもとになる情報と、前記第２の鍵のもとになる情報と少なくとも認証値とから所定の関数により生成された伝送用鍵のもとになる情報と、復号化側の復号化装置の固有ID情報と前記認証値とから生成された発行ID情報と、

を用いて前記コンテンツ情報を復号する方法であって、

前記固有ID情報と前記発行ID情報とから前記認証値を生成し、

少なくともこの生成した認証値と前記伝送用鍵のもとになる情報とをもとに、所定の逆関数により前記第２の鍵のもとになる情報を生成し、

この生成された第２の鍵のもとになる情報を用いて前記第２の鍵を生成し、この第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得、

この第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得る、
ことを特徴とするコンテンツ情報復号化方法。

（３）　暗号化されたコンテンツ情報を復号するための第１の鍵を生成するために必要な鍵生成情報を外部から得て前記第１の鍵を生成し、前記暗号化されたコンテンツ情報を復号する復号化装置において、

所定の認証値とこの復号化装置の固有ID情報とから生成された発行ID情報が供給され、前記固有ID情報と前記発行ID情報とから前記認証値を生成する認証値生成手段と、

前記鍵生成情報の少なくとも一部と少なくとも前記認証値とから所定の関数により外部で生成された伝送用鍵のもとになる情報が供給されると共に、少なくとも前記認証値生成手段で生成された認証値が供給され、所定の逆関数により前記鍵生成情報の少なくとも一部を生成する演算手段と、
を設けたことを特徴とするコンテンツ情報復号化装置。

（４）　第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、第２の鍵のもとになる情報から生成された第２の鍵を用いて前記第１の鍵のもとになる情報の少なくとも一部を暗号化した暗号化第１の鍵のもとになる情報と、前記第２の鍵のもとになる情報と少なくとも認証値とから所定の関数により生成された伝送用鍵のもとになる情報と、この復号化装置の固有ID情報と前記認証値とから生成された発行ID情報と、
を用いて前記コンテンツ情報を復号する復号化装置であって、

前記固有ID情報と前記発行ID情報とから前記認証値を生成する認証値生成手段と、

少なくともこの生成した認証値と前記伝送用鍵のもとになる情報とをもとに、所定の逆関数により前記第２の鍵のもとになる情報を生成する第２の鍵情報生成手段と、

この生成された第２の鍵のもとになる情報を用いて前記第２の鍵を生成し、この第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得る第１の鍵情報復号化手段と、

この復号された第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得るコンテンツ情報復号化手段と、
を設けたことを特徴とするコンテンツ情報復号化装置。

（５）　前記認証値生成手段に供給すべき前記発行ID情報をユーザー自身が入力するための発行ID情報入力手段を設けたことを特徴とする上記（３）または（４）記載のコンテンツ情報復号化装置。

（６）　前記発行ID情報は、暗号化コンテンツ情報供給側において、復号化側から供給された復号化装置の固有ID情報が正規の復号化装置の固有ID情報であるとの認定後に発行され復号化側に供給されるものであることを特徴とする上記（１）記載のコンテンツ情報復号化方法、または上記（２）記載のコンテンツ情報復号化方法、または上記（３）記載のコンテンツ情報復号化装置、または上記（４）記載のコンテンツ情報復号化装置、または上記（５）記載のコンテンツ情報復号化装置。

【０００６】

【発明の実施の形態】

図１に本発明のコンテンツ情報復号化装置の一実施例の概略構成を示す。なお、本説明においては、磁気記録媒体、光記録媒体、半導体メモリ等を記録媒体と呼び、光ケーブル、電線、無線伝送路等の信号を伝送する伝送媒体を伝送路と呼ぶこととする。

【０００７】

まず、記録側または送信側の説明をする。一方向性関数演算装置１は第１の鍵のもとになる情報から一方向性の関数を用いて第１の鍵（コンテンツ鍵）を作成する。その第１の鍵を用いて、暗号化装置２によりコンテンツ情報を暗号化する。

【０００８】

一方向性関数とは、一方向性ハッシュ関数とも表現でき、関数hとその定義域のある値xが与えられてh(x) = h(y)となるようなyを求めることが困難な関数のことである。コンテンツ情報はMPEGなどの所定の圧縮方式によって圧縮された後

、DESなどの暗号化方式により暗号化される。DES暗号化方式は１９７７年にアメリカ連邦政府標準に採用されたもので代表的な共通鍵暗号化方式で５６ビットの鍵を用いて６４ビット単位で暗号化復号化を行うブロック暗号化方式である。

【０００９】

暗号化は６４ビットの平分を３２ビットづつに分割して転置、置換、非線型関数、排他的論理和により構成されている。例えばDESの場合、暗号化鍵は５６ビット程度である。従って一方向性関数の出力ビット数が５６ビットになるような第１の鍵のもとになる情報は、例えば特定のシステム固有の５６ビットの情報としておく。

【００１０】

この第１の鍵のもとになる情報は、一方向性関数の内容が公開されていることを前提とするならば、記録媒体に記録する場合、もしくは伝送路に伝送する場合、何らかの暗号化されているのが望ましい。

【００１１】

そこで、第１の鍵のもとになる情報は、第２の鍵のもとになる情報から一方向性関数演算装置５により作成される第２の鍵を用いて、暗号化装置３により暗号化され、暗号化第１の鍵のもとになる情報となる。暗号化第１の鍵のもとになる情報が、記録もしくは伝送される。なお、暗号化第１の鍵のもとになる情報は、第１の鍵のもとになる情報が全て暗号化されたものでもよいし、部分的に暗号化されたものでもよい。

【００１２】

また、第２の鍵のもとになる情報を伝えるための伝送用鍵のもとになる情報が、第２の鍵のもとになる情報と認証値として入力された情報とから、関数ｆにより生成される。（関数ｆ演算装置４を使用。）

関数ｆは図２に示すように、例えば第２の鍵のもとになる情報と認証値情報との排他的論理和をとるような関数でもよい。第２の鍵のもとになる情報は、第１の鍵のもとになる情報とは別のシステム固有の５６ビットの情報とする。

【００１３】

なお、伝送用鍵のもとになる情報生成時には、認証値ばかりでなく、さらに別

情報（国、地域、空間を定義したリージョンに関する情報等）を付加して生成してもよい。この場合、再生側または受信側の正規のユーザーのみ、記録側もしくは伝送側と同じ別情報を共有化できるものとする。

また、暗号化するコンテンツ情報毎やコンテンツ情報の種類毎に認証値を変えてもよい。この場合、後述する発行ID情報がコンテンツ情報毎やコンテンツ情報の種類毎に異なるものとなり、コンテンツ情報を復号可能とする正規の条件をより細分化でき、不正な条件下でのコンテンツ情報を復号をより強力に防止できる。

【００１４】

記録もしくは伝送される情報は、暗号化されたコンテンツ情報（暗号化コンテンツ情報）、暗号化された第１の鍵のもとになる情報（暗号化第１の鍵のもとになる情報）、及び関数ｆによって第２の鍵のもとになる情報の値を変更された伝送用鍵のもとになる情報である。

【００１５】

次に、コンテンツ情報の復号を行う側である再生側または受信側の説明をする。再生側または受信側では、この復号化機器（再生機器）の固有ID情報（シリアルナンバー等）と後述する発行ID情報とから認証値生成器１１により、暗号化側で用いた認証値を生成する。再生機器の固有ID情報であるシリアルナンバーは、再生機器内の不揮発性メモリーに記録されているものとする。

【００１６】

ここで、発行ID情報について説明する。発行ID情報は暗号化コンテンツ情報供給側で生成されるものであり、認証値と、復号化側（再生側もしくは受信側）から与えられる復号化機器（再生機器）の固有ID情報（シリアルナンバー等）とから生成される。生成された発行ID情報は復号化側に送信される。

【００１７】

例えば、再生機器を使っているユーザーが自分の再生機器のシリアルナンバー（固有ID情報）をインターネットやはがき等を利用して、暗号化コンテンツ情報供給側にある所定のID発行センターに登録した後、ID発行センターにおいて発行ID情報が発行される。発行ID情報は、インターネットやはがき等を利用してID発

行センターからユーザーに通知される。

【００１８】

図３に示すように、シリアルナンバーと発行IDとの排他的論理和をとった結果が認証値になるように発行IDを決定する。例えば、シリアルナンバーが0xfafbfcfdで特定の認証子が0xaabbccddである場合、シリアルナンバー：0xfafbfcfdと0x50403020との排他的論理和をとることで特定の認証子：0xaabbccddとなるので、発行IDを0x50403020とする。

【００１９】

もし、復号化側（再生側もしくは受信側）で不正な発行ID情報を入力したならば、認証値が得られず第２の鍵のもとになる情報を生成できない。よって、暗号化第１の鍵のもとになる情報の暗号を解けないことになり、結果的に、暗号化コンテンツ情報の暗号を解けないことになる。

【００２０】

なお、ID発行センターにおける発行ID情報は、復号化側から供給された再生機器の固有ID情報が正規の再生機器の固有ID情報であるとの認定後に発行されるようにしてもよい。また、一つの認証値に対する発行ID情報の発行は、再生機器１台当たり原則として１回限りとするようにしてもよい。

【００２１】

発行ID情報はユーザーが自身が、リモコン、再生機器のパネルボタン、キーボード、所定のマンマシーンインターフェース等によって再生機器に入力するようにしてもよい。

【００２２】

再生側または受信側では、認証値生成器１１により生成した認証値と、伝送されてきた（または記録媒体から再生された）伝送用鍵のもとになる情報とから、逆関数ｆによって第２の鍵のもとになる情報を生成する（逆関数ｆ演算装置６を使用。）。記録側もしくは伝送側において、伝送用鍵のもとになる情報生成時に、前述したように別情報が用いられた場合には、この別情報をも用いて逆関数ｆによって第２の鍵のもとになる情報を生成する。（正規のユーザーのみ、再生側または受信側で、記録側もしくは伝送側と同じ別情報を共有化できるものとする

。）

【００２３】

生成された第２の鍵のもとになる情報から一方向性関数を用いて第２の鍵を生成する（一方向性関数演算装置７を使用）。この第２の鍵で、同じく伝送されてきた（または記録媒体から再生された）暗号化第１の鍵のもとになる情報を復号化装置８により復号する。

【００２４】

復号された第１の鍵のもとになる情報から一方向性関数を用いて第１の鍵を生成する（一方向性関数演算装置９を使用）。一方向性関数演算装置９で生成された第１の鍵を用いて、伝送されてきた（または記録媒体から再生された）暗号化コンテンツ情報を復号化装置１０により復号する。これによって、コンテンツ情報を再生することが可能となる。

【００２５】

暗号化されたコンテンツ情報は記録媒体に記録されて再生側もしくは受信側に供給されてもよいし、放送や通信によって再生側もしくは受信側に配信される形態でもよい。

【００２６】

このように、本実施例では、再生側もしくは受信側において発行ID情報として、暗号化コンテンツ情報供給側で生成された正規の発行ID情報を入力しなければ、第２の鍵のもとになる情報が得られず、暗号化第１の鍵のもとになる情報の暗号を解けないことになる。結果的に、暗号化コンテンツ情報の暗号を解けないことになる。従って、本実施例を用いれば、不正な条件下でのコンテンツ情報の再生をより確実に防止し、正規の条件下でのみコンテンツ情報の再生を可能とすることができる。

【００２７】

上述の説明では、説明を簡単なものとするために、正関数と逆関数とで同じ排他的論理和をとる関数ｆとしたが、この関数ｆは逆関数が論理的に構成されるものであれば何でもよい。また、各情報は計算上ここでは全て５６ビットとすることを前提にしているが、各情報が５６ビット以下の場合には上位ビットを０で埋

めてもよく、５６ビットを超える場合には、５６ビットを超える部分を無視してもかまわない。

【００２８】

なお、ここでは請求項における暗号化の階層を２段として説明したが、２段はN段として構成してもよい。また本願の方式は１段目からN段目のどの階層において適用してもよい。

【００２９】

【発明の効果】

以上のように、本発明によれば、再生側もしくは受信側（復号側）において発行ID情報として、暗号化コンテンツ情報供給側で生成された正規の発行ID情報を入力しなければ、第２の鍵のもとになる情報が得られず、暗号化第１の鍵のもとになる情報の暗号を解けないことになる。このことは、結果的に、暗号化コンテンツ情報の暗号を解けないことを意味する。従って、本発明を用いれば、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下でのみコンテンツ情報の再生（復号）を可能とすることができる。

【図面の簡単な説明】

【図１】

本発明の一実施例の概略構成を示す図である。

【図２】

関数ｆを説明するための説明図である。

【図３】

発行ID情報の生成方法を説明するための図である。

【符号の説明】

１，５，７，９　一方向性関数演算装置

２，３　暗号化装置

４　関数ｆ演算装置

６　逆関数ｆ演算装置

８，１０　復号化装置

１１　認証値生成器

【書類名】　　図面

【図１】

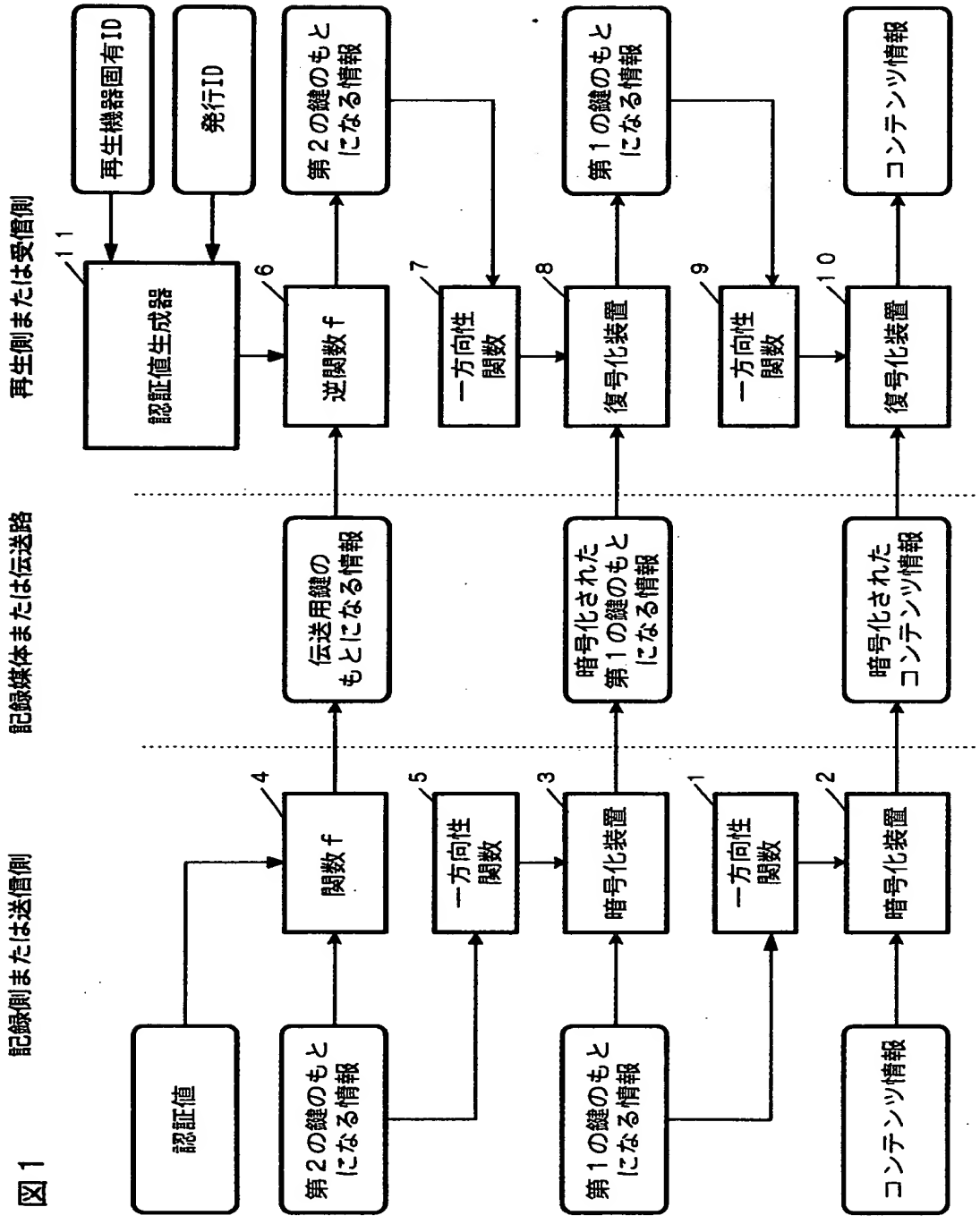

図１

【図２】

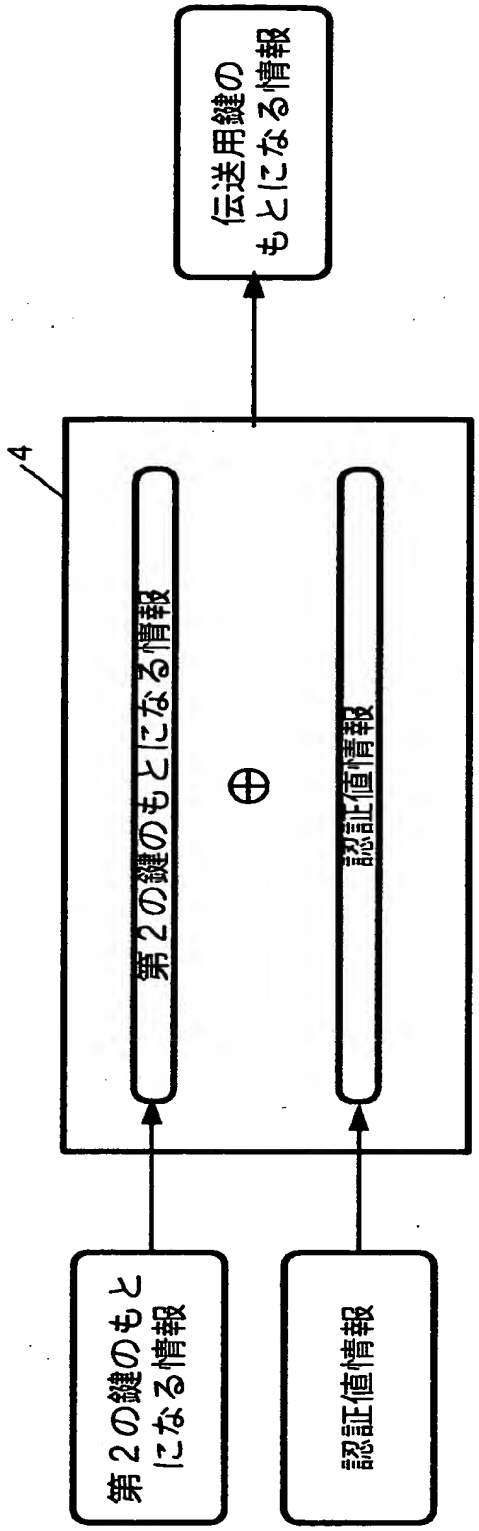

図２

【図３】

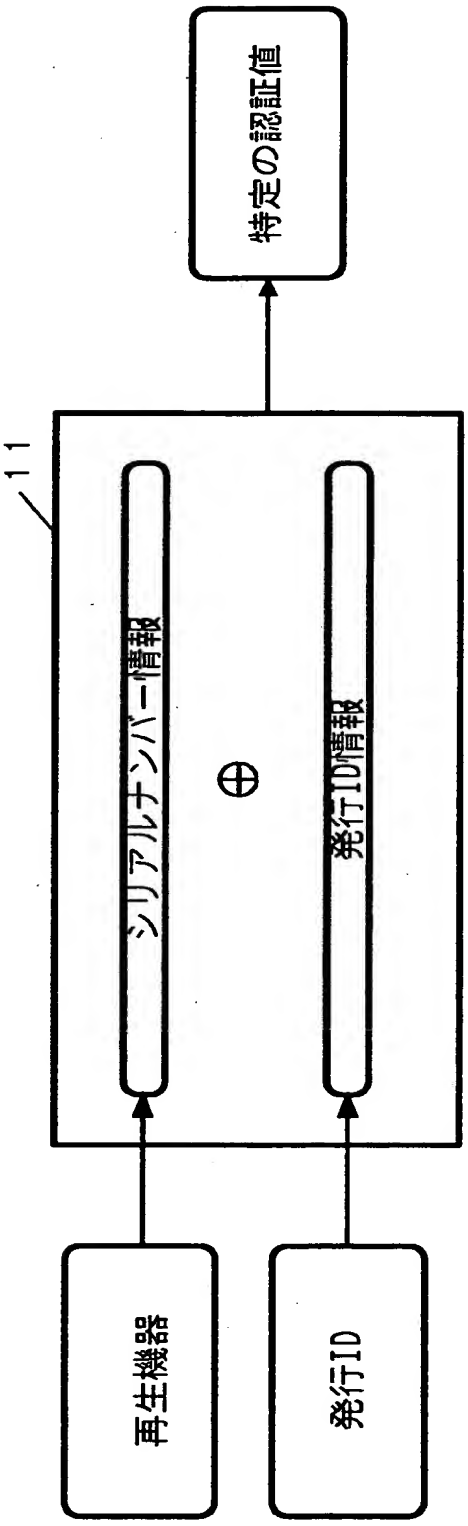

図３

【書類名】　　要約書

【要約】

【課題】　暗号化コンテンツ情報を正規の制限下においてのみ的確に再生（復号）することを可能とするコンテンツ情報復号化方法、復号化装置を提供すること。

【解決手段】　第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、第２の鍵のもとになる情報から生成された第２の鍵を用いて前記第１の鍵のもとになる情報の少なくとも一部を暗号化した暗号化第１の鍵のもとになる情報と、前記第２の鍵のもとになる情報と少なくとも認証値とから所定の関数により生成された伝送用鍵のもとになる情報と、復号化側の復号化装置の固有ＩＤ情報と前記認証値とから生成された発行ＩＤ情報とを用いて前記コンテンツ情報を復号する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社